

## AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method for providing security in a computer system by a clean group server, comprising:

~~selecting~~ specifying a set of properties for use in determining if an item is clean;

in response to receiving an add request from an item, the add request containing evidence collected from the item relating to the presence or absence of the properties in the specified set of properties, evaluating ~~an item~~ the add request to determine if ~~[[it]]~~ the evidence proves that the item has the specified set of properties; and

~~sending an add request to a clean group server; and~~

~~if the clean group server determines~~ determining from the evidence in the add request ~~[[that]]~~ whether the item has the specified set of properties, ~~the clean group server~~ and if so, designating the item as a member of a clean group by instructing a domain controller to add the item to the clean group, the domain controller configured to store information identifying network users and resources.

2. (Currently amended) The method of Claim 1, wherein the ~~items are computers~~ item is a computer.

3. (Currently amended) The method of Claim 2, wherein when ~~[[a]]~~ the computer is to be evaluated, a clean component is installed on the computer to perform compliance checks and to collect the evidence relating to the presence or absence of the properties in the specified set of properties.

4. (Original) The method of Claim 1, wherein a compliance check is performed at a selected time for an item to determine if the item has the specified set of properties.

5. (Original) The method of Claim 1, wherein one of the specified set of properties is whether all of the available updates have been installed.

6. (Original) The method of Claim 5, wherein the updates comprise at least one of security updates or service packs.

7. (Currently amended) The method of Claim ~~[[4]]~~ 1, ~~wherein if the compliance check fails, a message is sent to indicate~~ further comprising receiving a message sent by the clean component after the item fails a compliance check performed by the clean component, wherein the message indicates that the ~~object~~ item should not be in the clean group.

8. (Currently amended) The method of Claim 7, ~~wherein if the compliance check fails, the clean group membership of the item is invalidated~~ further comprising invalidating the clean group membership of the item in response to receiving the message.

9. (Currently amended) The method of Claim 8, wherein ~~the invalidation of~~ invalidating the clean group membership of the item comprises local actions including at least hiding the domain credentials of the item.

10. (Previously presented) The method of Claim 7, wherein if the compliance check fails, additional steps are taken including at least hiding cryptographic keys.

11. (Canceled)

12. (Currently amended) The method of Claim ~~[[11]]~~ 1, wherein after ~~a message is received and a determination is made that the item should be in~~ the item is designated as a member of the clean group, a countdown is started and if another message is not received by the end of the countdown, the item is removed from the clean group.

13. (Canceled)

14. (Currently amended) The method of Claim 1, ~~wherein the clean group server~~ initiates further comprising initiating a status check to determine if the ~~members~~ items in the clean group still have the specified properties.

15. (Currently amended) A system for managing security, comprising:

a clean group server;

a domain controller configured to store information identifying network users and resources, including a clean group indicating a group of computers and users that are more trusted than computers and users not included in the clean group;

~~an update component which includes updates for items;~~

a clean runtime component, the clean runtime component being installed on an item and being able to communicate with the ~~update component and the~~ clean group server; and

the clean runtime component ~~sending~~ configured to send an add request to the clean group server, the add request including evidence to be evaluated by the clean group server for determining whether to add the item to a clean group; [[and]]

[[if]] wherein the clean group server is configured to determine ~~that determine~~ whether the evidence sent by the [[item]] clean runtime component is sufficient to prove that the item has a specified set of properties is in compliance with a security policy, and if so, the clean group server to designates designate the item as a member of [[a]] the clean group by instructing the domain controller to add the item to the clean group.

16. (Canceled)

17. (Original) The system of Claim 15, wherein the items comprise computers.

18. (Currently amended) The system of Claim ~~[[17]]~~ 15, wherein the clean runtime component is configured to perform self-governance ~~compliance checks are performed for the items to determine if the items meet~~ item meets ~~[[the]]~~ selected criteria.

19. (Original) The system of Claim 18, wherein one of the criteria is whether selected available updates have been installed.

20. (Original) The system of Claim 19, wherein the updates comprise at least one of security updates or service packs.

21. (Currently amended) The system of Claim 18, wherein the clean runtime component is configured to, if a self-governance compliance check performed by the clean runtime component fails, send a message ~~is sent~~ from the clean runtime component to the clean group server to indicate that the item should not be in the clean group.

22. (Currently amended) The system of Claim 18, wherein ~~[[if]]~~ the clean runtime component is configured to send the add request to the clean group server only after the self-governance compliance check passes, ~~a message is sent from the clean runtime component to the clean group server to provide information that will be used to evaluate whether the item should be in the clean group.~~

23. (Currently amended) The system of Claim ~~[[22]]~~ 15, wherein ~~after a message is received to indicate that the item should be placed in~~ the clean group server is configured to, after designating the item as a member of the clean group, start a countdown; ~~is started~~ and if another ~~message~~ add request is not received by the end of the countdown, ~~the item is removed~~ clean group server is configured to remove the item from the clean group.

24. (Canceled)

25. (Currently amended) The system of Claim 15, wherein the clean group server ~~initiates~~ is configured to initiate a compliance check for items to determine if they should remain in the clean group.

26. (Currently amended) One or more computer-readable media having computer-executable components for providing security in a computer system, the computer-executable components comprising:

a clean runtime object for installation on a computer, wherein the clean runtime object, when executed, performs a compliance check to ~~determines~~ determine if the computer has a specified set of properties, and sends an add request containing evidence relating to whether the computer has the specified set of properties to a clean group server; and

instructions for installation on a clean group server for processing the add request, wherein the instructions, when executed, cause the clean group server to ~~designate~~ instruct a domain controller configured to store information identifying network users and resources to add the computer as a member of a clean group upon receipt of an add request, if the clean group server determines that the add request ~~is valid~~ contains sufficient evidence to prove that the computer has the specified set of properties.

27. (Original) The media of Claim 26, wherein the compliance check is performed initially upon installation of the runtime object.

28. (Currently amended) The media of Claim 26, wherein the ~~compliance check comprises a determination of~~ evidence indicates whether ~~selected~~ specified available updates have been installed on the computer.

29. (Currently amended) The media of Claim 28, wherein the ~~selected~~ specified available updates comprise at least one of security updates or service packs.

30. (Currently amended) The media of Claim 26, wherein after the add request is received by the clean group server, a countdown is started and if another message is not received by the end of the countdown, the clean group server instructs the domain controller to remove the computer is removed as a member of from the clean group.

31. (Previously presented) The media of Claim 26, wherein the clean runtime object initiates a compliance check on the computer.

32. (Previously presented) The media of Claim 26, wherein the clean group server communicates with the runtime object to initiate a compliance check.

33. (Currently amended) A method for providing security in a computer system, comprising:

~~selecting~~ specifying a set of properties for use in determining if a computer is clean;

evaluating a computer to determine if it has the specified set of properties;

sending an add request to a clean group server; and

based on whether or not the clean group server determines that the computer is in compliance, the clean group server disabling or enabling the computer domain account on a domain controller, the domain controller configured to store information identifying network users and resources.

34. (Currently amended) The method of Claim 33, wherein when a new computer domain account is to be added to the domain ~~account~~, the new ~~computer's~~ domain account is placed in a disabled state until the associated computer is proved to the clean group server to be in compliance.

35. (Currently amended) The method of Claim 33, wherein when a new computer domain account is to be added to the domain ~~account~~, the domain join operation that creates the new computer domain account is predicated on proving that the computer is in compliance by requiring the clean group server to participate in the domain join operations.

36. (Previously presented) The method of Claim 33, wherein evaluating a computer comprises determining whether available updates have been installed on the computer.

37. (Original) The method of Claim 33, wherein the computer periodically performs compliance checks.

38. (Previously presented) The method of Claim 33, wherein the clean group server periodically initiates a compliance check on the computer.

39. (Currently amended) A method for providing security in a computer system, comprising:

performing compliance checks for items;

placing items which pass the compliance check into a clean group by communicating with a domain controller, the domain controller configured to store information identifying network users and resources; and

removing items from the clean group which fail the compliance check;

wherein items within the clean group can access a collection of IPSec communication requirements and parameters that allow them to communicate with other items within the clean group; and

items not within the clean group cannot access the collection of IPSec communication requirements and parameters, and are thereby quarantined from receiving information from or sending information to items within the clean group.

40. (Original) The method of Claim 39, wherein after an item passes a compliance check and is placed in the clean group, a countdown is started and if another compliance check is not passed by the end of the countdown, the item is removed from the clean group.

41. (Original) The method of Claim 39, wherein the item is a computer.

42. (Original) The method of Claim 39, wherein the item performs a compliance check.

43. (Original) The method of Claim 39, wherein a clean group server initiates a compliance check on the item.

44. (Original) The method of Claim 39, wherein the compliance check is performed by the item communicating with an update Web site to determine if updates are available for the item.

45. (Original) The method of Claim 44, wherein the item communicates with a clean group server to establish its membership in the clean group.

46. (Canceled)

47. (Previously presented) The method of Claim 39, wherein a compliance check is initiated by one or more of a client coming online, changes in client status/configuration, changes in network status/configuration, or changes to a compliance policy.

48. (Original) The method of Claim 39, wherein a clean group server communicates to non-compliant items how to get back into compliance.



49. (Original) The method of Claim 48, wherein the non-compliant items are directed to a Web site with online instructions to the user, and once the instructions are followed, another server-assisted compliance check is initiated.

50. (Original) The method of Claim 48, wherein the non-compliant items are instructed how to get into the compliant state automatically without requiring a user's involvement.

51. (Currently amended) The method of Claim 39, wherein an item is a user, and a user's clean group membership is evaluated on the basis of whether ~~the user's computer~~ each of a set of computers associated with the user is in compliance.

52. (Canceled)

53. (Previously presented) The method of Claim 39, wherein items within the clean group are given access to the collection of IPSec settings by binding active directory group policy to the clean group membership such that only members of the clean group can read the policy.

54-55. (Canceled)

56. (Previously presented) The method of Claim 39, wherein a client that changes state from membership in the clean group to non-membership is required to clear all policy settings distributed via the clean group.

57-59. (Canceled)

60. (Currently amended) The method of Claim 1, ~~wherein~~ further comprising designating the item as a member of a dirty group if the clean group server determines that the

item does not have the specified set of properties, ~~the clean group server designating the item as a member of a dirty group.~~

61. (Currently amended) The system of Claim 15, wherein ~~if the clean group server determines that the item does not have the specified set of properties,~~ the clean group server is further configured to designate ~~designating~~ the item as a member of a dirty group if the evidence sent by the clean runtime component is insufficient to prove that the item is in compliance with the security policy.

62. (Currently amended) The method of Claim 8, wherein ~~the invalidation of~~ invalidating the clean group membership of the item comprises local actions including at least erasing the domain credentials of the item.

63. (Previously presented) The method of Claim 7, wherein if the compliance check fails, additional steps are taken including at least logging out a privileged user.